

Docket No. AUS920010942US1

CLAIMS:

What is claimed is:

1. A method of controlling access to computer system
5 resources based on permissions, comprising:
 receiving a request for access to a computer system
 resource and
 executing, on the request, a security policy
 identified by a security policy file class,
10 wherein the security policy determines if a
 superclass permission is implied by a required permission
 in each protection domain of an access control context
 and adds the required permission to a permission
 collection if the superclass permission is implied by the
15 required permission in each protection domain of the
 access control context, and wherein the security policy
 grants access to the computer system resource if the
 superclass permission of the required permission is
 present in each protection domain of the access control
20 context.
2. The method of claim 1, wherein the request is
 received from bytecode.
- 25 3. The method of claim 1, further comprising:
 determining the required permission based on a
 CodeSource associated with the request.
4. The method of claim 1, wherein the security policy
30 determines if a superclass permission is implied by a
 required permission in each protection domain by
 determining if at least one permission collection in each
 protection domain includes the superclass permission.

Docket No. AUS920010942US1

5. The method of claim 1, wherein the security policy adds the required permission to a permission collection by creating a new permission collection and adding the
5 required permission to the new permission collection.

6. The method of claim 5, wherein the security policy adds the required permission to a permission collection by adding any subclass permissions of the required
10 permission to the new permission collection.

7. The method of claim 1, further comprising retrieving the access control context for a thread of execution that sent the request for access to the computer system
15 resource.

8. The method of claim 1, wherein the security policy adds the required permission to a permission collection by adding the permission to a permission collection
20 associated with the superclass permission.

9. A computer program product in a computer readable medium for controlling access to computer system resources based on permissions, comprising:
25 first instructions for receiving a request for access to a computer system resource; and
second instructions for executing, on the request, a security policy identified by a security policy file class,
30 wherein the security policy includes instructions for determining if a superclass permission is implied by a required permission in each protection domain of an access control context and instructions for adding the

Docket No. AUS920010942US1

required permission to a permission collection if the superclass permission is implied by the required permission in each protection domain of the access control context, and wherein the security policy further includes instructions for granting access to the computer system resource if the superclass permission of the required permission is present in each protection domain of the access control context.

10 10. The computer program product of claim 9, wherein the request is received from bytecode.

11. The computer program product of claim 9, further comprising:

15 third instructions for determining the required permission based on a CodeSource associated with the request.

12. The computer program product of claim 9, wherein the instructions in the security policy for determining if a superclass permission is implied by a required permission in each protection domain include instructions for determining if at least one permission collection in each protection domain includes the superclass permission.

25 13. The computer program product of claim 9, wherein the instructions in the security policy for adding the required permission to a permission collection include instructions for creating a new permission collection and
30 instructions for adding the required permission to the new permission collection.

Docket No. AUS920010942US1

14. The computer program product of claim 13, wherein the instructions in the security policy for adding the required permission to a permission collection include instructions for adding any subclass permissions of the
5 required permission to the new permission collection.

15. The computer program product of claim 9, further comprising third instructions for retrieving the access control context for a thread of execution that sent the
10 request for access to the computer system resource.

16. The computer program product of claim 9, wherein the instructions in the security policy for adding the required permission to a permission collection include
15 instructions for adding the permission to a permission collection associated with the superclass permission.

17. An apparatus for controlling access to computer system resources based on permissions, comprising:
20 means for receiving a request for access to a computer system resource; and
means for executing, on the request, a security policy identified by a security policy file class,
wherein the security policy determines if a
25 superclass permission is implied by a required permission in each protection domain of an access control context and adds the required permission to a permission collection if the superclass permission is implied by the required permission in each protection domain of the
30 access control context, and wherein the security policy grants access to the computer system resource if the superclass permission of the required permission is

Docket No. AUS920010942US1

present in each protection domain of the access control context.

18. The apparatus of claim 17, wherein the request is
5 received from bytecode.

19. The apparatus of claim 17, further comprising:
means for determining the required permission based
on a CodeSource associated with the request.

10

20. The apparatus of claim 17, wherein the security
policy determines if a superclass permission is implied
by a required permission in each protection domain by
determining if at least one permission collection in each
15 protection domain includes the superclass permission.

21. The apparatus of claim 17, wherein the security
policy adds the required permission to a permission
collection by creating a new permission collection and
20 adding the required permission to the new permission
collection.

22. The apparatus of claim 21, wherein the security
policy adds the required permission to a permission
25 collection by adding any subclass permissions of the
required permission to the new permission collection.

23. The apparatus of claim 17, further comprising means
for retrieving the access control context for a thread of
30 execution that sent the request for access to the
computer system resource.

[illegible]